云计算环境下国家学术信息资源安全控制与管理*

■ 万莉[1] 胡昌平[2]

[1] 南昌大学新闻与传播学院 南昌 330031 [2] 武汉大学信息管理学院 武汉 430072

摘要：［目的/意义］构建云计算环境下国家学术信息资源安全控制框架，为云计算环境下国家学术信息资源安全保障提供参考。［方法/过程］在借鉴传统复杂系统安全控制论的人、机、环有机整体以及信息保障技术框架(IATF)的人、操作、技术的模式基础上，结合云计算环境下信息安全控制关键域与治理域，构建云计算环境下国家学术信息资源安全控制框架。［结果/结论］云计算环境下国家学术信息资源安全涉及关键领域包括全员管理、控制策略、安全测评，云计算环境下国家学术信息资源安全控制框架既包括云计算环境下国家学术信息资源安全控制措施，同时包括对其安全控制措施的有效性测量。

关键词：学术信息资源 安全控制 安全管理 信息资源安全

分类号：G250

DOI：10.13266/j.issn.0252－3116.2019.07.001

1 引言

目前，针对云计算环境下学术信息资源安全控制的研究较为匮乏，需要通过对国内外云计算环境下信息安全控制的梳理以及结合学术信息资源特征，构建云计算环境下国家学术信息资源安全控制的框架，从而提出针对云计算环境下国家学术信息资源安全保障的管理与控制策略。云计算环境下信息安全控制的研究主要集中以下几个方面：

1.1 信息安全控制标准及控制分类研究

美国国家标准与技术研究院(National Institute of Standard and Technology，NIST)对信息安全控制进行了深入的研究，NIST SP800系列已经成为美国指导信息安全建设的主要标准，应用于金融、国防、医疗等不同领域，是一套相对成熟的安全控制体系[1]。ISO/IEC JTC 1技术委员会制定的ISO/IEC 27003标准《信息技术－安全技术 信息安全管理体系实施指南》，旨在支持信息安全管理的过程，确保相关利益方的信息资产满足组织所定义的可接受的风险级别[2]。以上信息安全标准对云计算环境下信息安全控制具有重要参考作用。美国标准与技术研究院特别出版物SP800－53中指出安全控制需要对信息系统进行安全分类，从安全分类中确定信息系统影响等级，然后应用相关标准措施中基准安全控制的控制集。美国标准与技术研究院特别出版物SP800系列主要涉及计算机安全领域的热点研究，美国国家标准与技术研究所定义的控制可以分为：技术、运营、管理三大种类，安全控制则由三大种类细化成18个系列组成[3]。美国标准与技术研究院特别出版物800－53 r4细化的安全控制涉及政策、监督、个人行为、人员操作、信息系统等多方面。安全控制集包括访问控制、意识与培训、审计和责任追究、安全评估与授权、应急计划、事故响应、人员安全、风险评估、系统和信息完整性等[4]。

1.2 针对云业务的安全控制研究

ISO/IEC 27017《信息技术－安全技术－基于ISO/IEC 27002的云服务信息安全控制的实用规则》云安全控制标准为云服务提供商提供了安全云服务的发展方向，是云服务提供商接受保护控制的标准文件，提出控制模式以解决云服务面临的风险[5-6]。美国政府提出的“联邦风险和授权管理项目”(FedRAMP)定义了云计算安全控制方面的需求，主要涵盖了漏洞扫描、冲突监控、日志及记录4个方面[7]。云安全联盟发布了云安全控制矩阵，用以满足云行业信息安全需求。云安全控制矩阵基于生命周期定义了安全控制规划、实施、

* 本文系国家社会科学基金重大项目“云环境下国家数字学术资源信息安全保障体系研究”(项目编号:14ZDB168)研究成果之一。
作者简介：万莉(ORCID:0000－0001－6178－1435)，讲师，博士，E-mail:towanli@126.com；胡昌平(ORCID:0000－0002－9491－2160)，教授，博士生导师。
收稿日期:2018－07－16 修回日期:2018－10－27 本文起止页码:5－14 本文责任编辑:王传清

评估、维护,用于指导不同阶段的安全控制以及不同领域安全控制的选择[8]。

基于不同领域的安全控制,更接近于最佳实践以及有效实现云安全保障。然而并不是越复杂的安全控制越好,云安全控制的优化目标在于采用简单但行之有效的安全控制措施。因此,应当实施合理的、具有成本效益的安全控制。此外,面临新漏洞和攻击等不断涌现出新的挑战,需要持续改善安全,披露新漏洞并进行补救,而且必须不断地审查安全控制和程序,持续进行改进,从而支持任务变化以及应对不断变化的威胁[8]。对于云计算环境下不同阶段以及不同领域都应该制定相对应的安全控制措施,以降低云计算环境下信息安全面临的安全风险。

1.3 不同的云服务交付模式下的安全控制研究

云安全联盟(Cloud Security Alliance,CSA)发布的“一致性评估倡议调查问卷”(Consensus Assessments Initiative Questionnaire,CAIQ)专注于提供行业认可的方式来记录 IaaS、PaaS、SaaS 提供的产品的安全控制,且保障了安全控制的透明性[9]。CSA 构建了云服务安全参考模型:将 IaaS、PaaS、SaaS 云服务模型与安全控制和合规模型进行映射[10]。安全控制模型包括:应用程序、数据信息、管理、网络、可信计算、计算和存储、物理层,从安全控制方面描述了云服务安全控制涉及的重点。从不同云服务交付模式的角度,为国家学术信息资源云服务安全控制提供了参考。

从本质上来讲,安全控制是安全保障的对策或措施,通过对安全风险进行预防、阻止、应对、响应等进行安全保障。控制的分类具有多样性,需要根据不同的安全控制对象制定方案,通常涉及到技术、管理、运营等多个类别。传统安全控制已形成较为成熟的理论并进行了相应的实践,为云计算环境下的信息安全控制奠定了基础,云计算环境下国家学术信息资源安全控制需要在借鉴传统安全控制的基础上进行拓展。总体上看,传统的安全控制的探索为云计算环境下国家学术信息资源安全控制的研究奠定了基础,从安全控制结构、安全控制技术、安全控制措施等方面可以为云计算环境下国家学术信息资源安全控制体系的构建提供参考。云计算环境下安全控制需要在借鉴传统 IT 环境中的安全控制机制基础上,结合云计算环境下特有的信息安全风险,围绕云安全的关键域提出安全控制建议,以期为用户提供安全的云服务。由于不是简单移植传统网络环境下的安全技术保障措施,故需要研究云计算特有的关键安全风险问题。

2 云计算环境下国家学术信息资源安全控制框架构建

云计算环境下国家学术信息资源云服务建设面临着不同的云服务交付模式与云服务部署模式的选择,目前云产品也已经呈现不同的消费模式组合及服务形态的变化。不同的消费模式以及云服务形态,其安全风险和安全控制范围与职责存在较大差异[11]。云计算环境下国家学术信息资源的云服务部署模式按照云服务部署模式的类型可以划分为:公有云、私有云/社区云、混合云。云计算环境下国家学术信息资源采用混合云服务部署模式。混合云部署模式下基础设施由两个或多个云进行共享,在资源共享过程中需要进行跨云的调度。云计算环境下国家学术信息资源云服务需要在公有云部分和私有云部分进行访问,安全控制的难度较其他云服务部署模式大。云计算环境下国家学术信息资源安全控制不是简单的基于云安全技术的安全解决方法,需要针对云计算环境下国家学术信息资源安全特征与问题进行相应的安全控制。

不同的云服务交付模式层次,云服务提供商和用户所承担的信息安全保障责任与范围也各不相同。在 IaaS 模式下,主要由云服务提供商进行安全控制,保障底层基础设施和抽象层的安全防护。在 PaaS 环境下,安全控制的范围介于 IaaS 与 SaaS 之间,平台本身的安全控制由云服务提供商提供,而云用户需要负责所开发的云应用的安全。在 SaaS 环境下,安全控制范围及相关措施可以通过服务等级协议(service level agreement,SLA)进行确认,SLA 内容由云用户和云服务提供商进行协商,对双方所承担的安全控制责任进行划分与约束。通过三种云服务交付模式的对比,可以看到云服务的层次越高,云服务提供商安全控制的责任越大,用户对云服务提供商安全控制的依赖程度也越高。

在云计算环境下不是所有的安全需求都是等同的,基于不同的安全需求以及信息系统,安全控制的重点也不一样。对于云计算环境下国家学术信息资源公有云部分,在保密性方面的安全控制更加强调完整性和可用性。云计算环境下国家学术信息资源私有云部分,在保密性方面的安全控制更加强调保密性和可行性。因此,云计算环境下国家学术信息资源安全控制可以根据不同的云服务部署模式进行优先级以及基准配置。

云计算环境下国家学术信息资源安全保障是一项复杂的系统工程,层次结构以及信息、能力交互错综复

杂。复杂系统功能本质安全在于实现系统结构本质安全,维护系统结构和系统边界的稳定性,以及微观层面信息、能力交互过程中的人、机、环的安全。针对传统环境下的信息安全保障的问题与实践,信息保障技术框架(Information Assurance Technical Framework,IATF)提出了信息安全保障的建议和指南,IATF从安全控制结构、安全控制技术、安全控制措施等为云计算环境下国家学术信息资源安全控制体系构建提供了参考。在借鉴传统复杂系统安全控制论的人、机、环有机整体以及IATF的人、操作、技术的模式基础上,结合云计算环境下信息安全控制关键域与治理域,构建云计算环境下国家学术信息资源安全控制框架,见图1[10,12-14]。突出国家学术信息资源云平台建设所涉及的全员管理、风险管理、安全基线建设、应急响应、合规审计、信息安全测评等关键方面的安全控制。云计算环境下国家学术信息资源安全控制既包括云计算环境下国家学术信息资源安全控制措施,同时包括对云计算环境下国家学术信息资源安全控制措施的有效性测量。

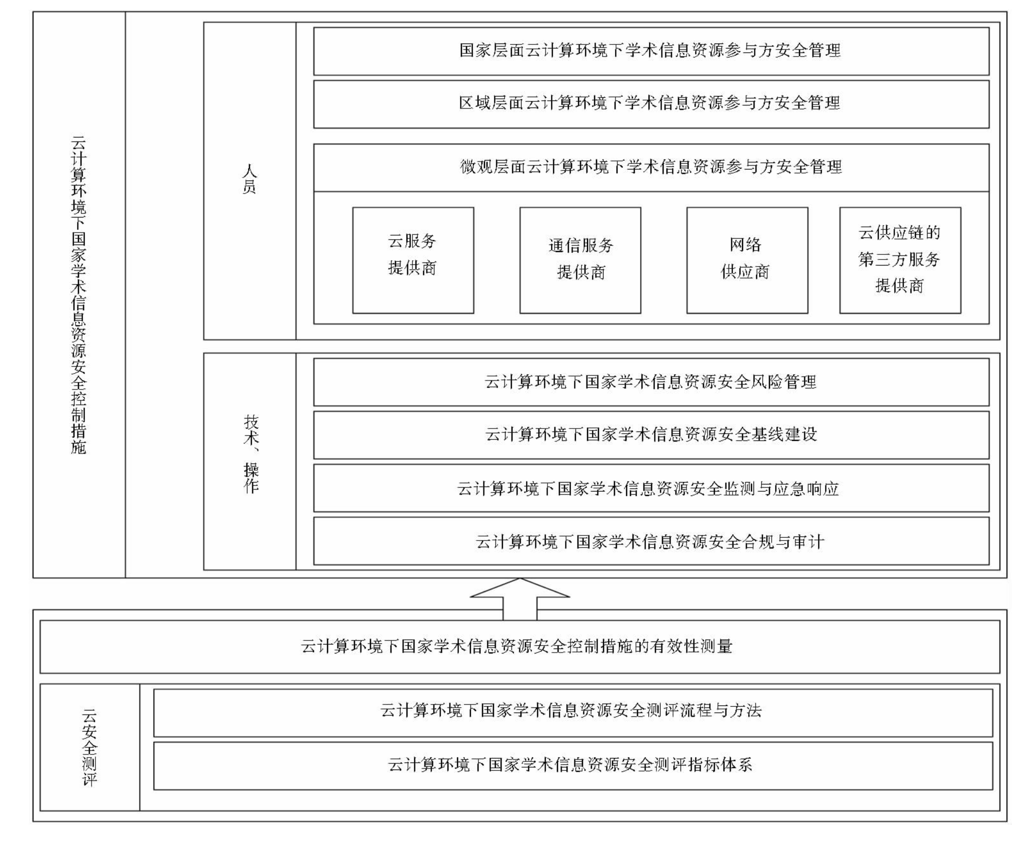


图1　云计算环境下国家学术信息资源安全控制框架

3　云计算环境下国家学术信息资源全员安全管理

国家学术信息资源云平台建设涉及的主体众多。以CALIS为代表的国家学术信息资源云平台建设,支持各个图书馆之间的服务整合,在此基础上提供新的服务体系。CALIS数字图书馆云服务平台在IaaS、HaaS、PaaS基础上构建SaaS服务,并通过CALIS数字图书馆云服务平台将第三方服务进行整合,构建CALIS云服务中心,同时面向各个图书馆提供SaaS云服务。国家学术信息资源云平台面向资源共享共建,为用户提供高效率、可扩展的云计算服务。国家层面的学术信息资源云平台建设需要政府信息科学规划以及各级相关部门的协同组织。需要依托网络以及区域将国家层面的学术信息资源云平台建设逐层细化实施,在区域范围实现学术信息资源的共享共建,依托区域节点实现学术信息资源的整合从而更好地为学术信息资源用户提供学术信息资源云服务。云计算环境下国家学术信息资源安全保障不仅需要学术信息资源服务机构和云服务提供商之间协调工作,而且需要各个学术信息资源服务机构、国家信息服务管理机构之间权责分明,针对云计算环境下国家学术信息资源安全的统筹管理。

3.1 国家层面云计算环境下学术信息资源参与方安全管理

云计算环境下国家学术信息资源安全是国家信息安全的重要组成部分。云计算环境下国家学术信息资源建设面向共享共建,资源相对集中,一旦国家学术信息资源云平台被破坏,那么会威胁到众多的学术信息资源服务机构。如果攻击者利用云平台的漏洞窃取、修改、删除等破坏存储在云端的学术信息资源,不仅会给学术信息资源领域造成损失,甚至还可能会威胁国家安全。因此,云计算环境下国家学术信息资源安全依赖国家的宏观指导,对国家学术信息资源云服务实施管理与监督。

我国对信息安全保障非常重视,成立了国家信息化领导小组进一步加强我国信息化建设以及维护国家信息安全,在具体实施过程中主要通过国家信息服务管理协调委员会进行实际工作的管理。国家信息服务管理协调委员会对云计算环境下国家学术信息资源云服务涉及的学术信息资源服务机构进行统筹分工,明确各个机构的职责,制定学术信息资源服务机构协调合作的方针。

基于国家层面的云计算环境下国家学术信息资源安全管理,可以有效地控制国家学术信息资源共享共建所面临的组织障碍以及不同地域之间进行资源整合的地域障碍。从国家层面将国家学术信息资源云服务的总体组织结构进行规划,可以进一步明确国家学术信息资源共享共建的资源组织与调度,在合作分工以及组织协同的基础上加强云计算环境下国家学术信息资源的安全保障。同时,通过建立针对云计算环境下国家学术信息资源云服务建设的监督机构,对云计算环境下国家学术信息资源安全进行监督。出台相应的标准、法律法规可进一步规范云服务行业和云服务提供商的行为。

3.2 区域层面云计算环境下学术信息资源参与方安全管理

区域层面的云计算环境下学术信息资源参与方安全管理主要涉及中观层面,按照国家层面的云计算环境下国家学术信息资源安全指导方针,构建区域学术信息资源云服务中心,制定细化的区域学术信息资源安全管理的方针,面向不同学术信息资源服务机构进行分工与协调,同时对云服务提供商和云服务行业加强监管。

我国在传统网络环境下的学术信息资源共享共建已经开展了实践工作,在学术信息资源共享共建参与方的管理上已经积累了经验。广东省立中山图书馆作为发起组织,构建了由国内众多公共图书馆参与服务的联合参考咨询网,面向用户提供参考咨询和文献传递服务[15]。广东省的参考咨询服务于2001年开通,联合了商业学术信息资源提供商和国内外多家图书馆。2003年构建自己的网上参考咨询平台,并逐步实现了资源的共享共建以及面向用户的学术信息资源服务开放。在建设过程中,广东省为省域学术信息资源共享共建提供了必要的政策和管理支持,成立了广东省跨系统联合数字参考咨询指导委员会,该委员会负责规范、标准体系的建设,相关政府部门负责监督和协调跨系统联合数字参考咨询服务过程中的各个机构,为区域学术信息资源共享共建参与方的管理提供了参考[16]。

区域层面云计算环境下学术信息资源参与方的管理需要成立负责区域学术信息资源安全的管理部门,设置区域学术信息资源安全管理小组负责该区域内云计算环境下学术信息资源建设的组织管理工作,主要涉及制定共享共建的管理规范、明确各个学术信息资源服务机构在共享共建及云服务过程的职责、学术信息资源服务机构的协同分工等,面向区域的学术信息资源云服务建设,打破了传统网络环境下学术信息资源各自为政的局面[17]。成立区域学术信息资源云服务技术小组,可为云计算环境下学术信息资源服务机构遇到的技术应用问题提供指导,并且制定了云计算环境下学术信息资源建设的标准体系,如:云应用开发标准、元数据标准、服务标准等,突出了技术难题的解决。成立区域学术信息资源云服务资源管理小组,主要负责区域学术信息资源共享共建的云服务中心资源调度,制定统一的工作规范,按照规定流程对各个学术资源机构的学术信息资源数据进行组织和配置,并对学术信息资源的质量和使用情况进行监督。成立学术信息资源云服务审计和监督小组,负责区域学术信息资源云服务建设过程中的安全监督与审计工作,主要负责对云计算环境下学术信息资源建设过程中的各种操作和安全事件监督,以及对制定的管理规范、控制策略等信息安全进行评估,不断完善云计算环境下学术信息资源安全体系。此外,成立专家指导小组,选取学术信息资源服务机构、相关政府部门、云服务提供商等相关参与方的专家对云计算环境下学术信息资源建设过程中的问题提供建议,不断增强和促进云计算环境下学术信息资源安全控制。区域层面的云计算环境下国家学术信息资源参与方安全管理体系结构,见图2。

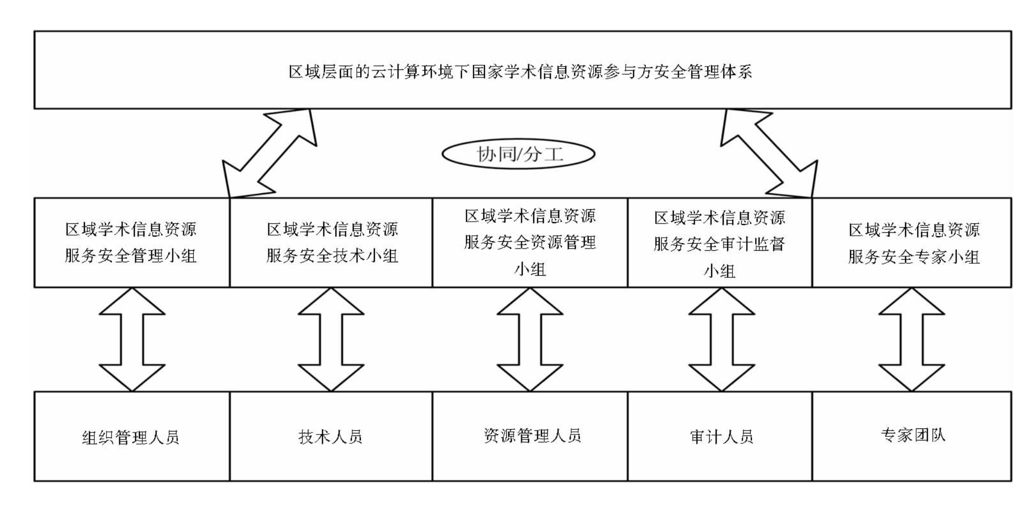


图 2　区域层面的云计算环境下国家学术信息资源参与方安全管理体系结构

3.3　微观层面云计算环境下学术信息资源参与方安全管理

微观层面的云计算环境下国家学术信息资源服务参与方主要涉及学术信息资源服务机构、云服务提供商、网络运营商、通信服务商、云供应链上的其他服务提供商等，见图 3。网络运营商主要为学术信息资源服务机构提供网络连接服务并提供一定的网络安全保障。云计算环境下学术信息资源服务机构必须通过网络才能利用云计算服务。为了适应学术信息资源服务机构的弹性需求，支持云服务功能的虚拟机需要重新创建和迁移，这使得在迁移的过程中虚拟机相对容易受到攻击，需要网络运营商、通信服务商与云服务提供商共同参与学术信息资源的安全防护与控制。

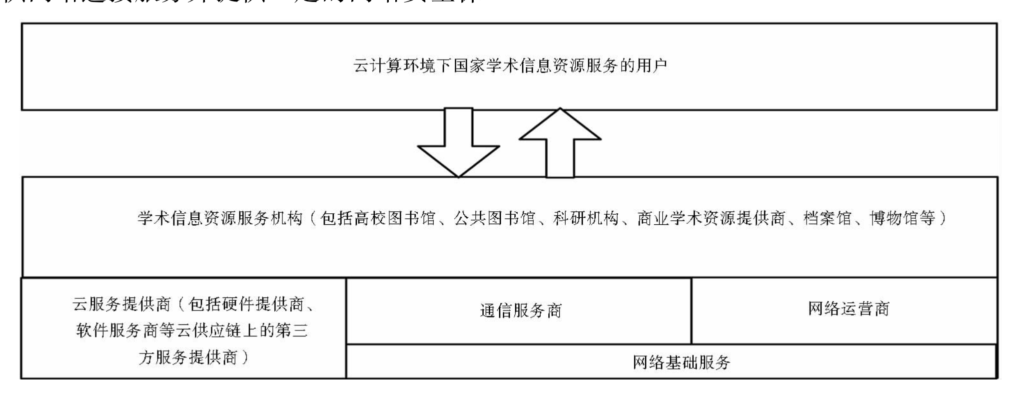


图 3　微观层面的云计算环境下学术信息资源服务参与方结构

学术信息资源服务机构使用云计算服务、通信服务、网络服务等，都需要通过服务提供商购买所需服务，从而形成了直接的买卖关系。在交易过程中，买卖双方会对安全问题产生共识，通过合同契约对双方进行约束。微观层面上的学术信息资源云服务参与方管理的重点在于构建学术信息资源服务机构以及服务提供商之间的信任关系。在学术信息资源云服务建设过程中，可通过与其他参与方建立可靠的信任关系，建立一定的约束机制来约束各参与方责任与义务，促使学术信息资源云服务领域各个参与方按照预定目标进行合作以实现预期的目标。无论是在云计算环境下还是在网络环境下，通过用户与服务提供商协定来缔结契约，都是对服务提供商和用户进行管理的有效方法。服务等级协议（service level agreement，SLA）是服务提供商和用户经协商确定服务等级协议或合同，通过合同对双方的义务、责任等达成共识，以达到持续服务的目标，在云计算环境下利用 SLA 是实现国家学术信息资源云服务参与方信任管理的重要手段。

4　云计算环境下国家学术信息资源安全全程控制策略

云计算环境下国家学术信息资源安全全程控制策略，主要围绕云计算环境下国家学术信息资源的安全风险管理、安全基线建设、安全监测与应急响应、安全

合规审计开展研究。

4.1 云计算环境下国家学术信息资源安全风险管理

云计算环境下国家学术信息资源系统仍然面临着信息系统客观存在的安全风险，可以通过对安全风险进行评估，从而采取有针对性的有效控制措施。风险控制是云计算环境下国家学术信息资源安全控制的关键组成部分，需要将国家学术信息资源云服务信息系统的安全风险限制在可控范围内，增强云计算环境下国家学术信息资源的安全保障。云计算环境下国家学术信息资源安全风险管理所遵循的思路在于，根据国家学术信息资源的分布，确定风险域以及风险因素，通过对风险因素的观测和采集，采用量化工具进行分析，在风险评估的基础上，进行安全策略和安全措施的制定，有效地控制风险[18]。

被控云信息系统是网络、人员、运行环境、业务应用要素的集合，由于云计算环境下信息安全风险、资产脆弱性以及安全风险的存在，需要通过对安全风险进行观测和评估，将安全风险变成可控安全风险，将残余安全风险经过再一次的循环进行观测、评估以制定安全控制策略。在此基础上不断改进安全控制策略以降低安全风险，经过循环操作，直到最终输出的安全风险都在可接受的范围内。风险评估过程一般包括风险识别、风险分析和风险评价等一系列环节，风险分析则包括资产、威胁、脆弱性等方面。首先对资产类别、资产价值进行判断，之后对威胁发生的类型、频率进行分析，再根据脆弱性程度进行赋值，最后在综合验证资产价值、威胁频率、脆弱性的基础上，预估安全事故可能发生的概率以及可能造成的损失。

4.2 云计算环境下国家学术信息资源安全基线建设

云计算环境下国家学术信息资源云服务平台的构建涉及多元主体，众多学术资源机构如果采用不同的云服务提供商提供的云服务，需要应对网络结构复杂、服务器种类繁多等诸多问题。因此，国家学术信息资源的云服务过程中不能仅仅基于传统的信息系统的方式对云信息系统进行维护，而忽略云计算环境下国家学术信息资源安全控制的特点与需求。因此，云计算环境下国家学术信息资源安全的保障必须建立相关的基线规范，基于相关的基线规范实施安全控制。

美国启动联邦风险与授权管理项目(FedRAMP)进行云安全管理研究，期望在风险控制的基础上充分利用云安全的优势。在云计算安全管理体系构建的过程中突出了云安全控制基线的建设，制定了《FedRAMP云安全控制措施》，为我国云计算环境下国家学术信息资源安全基线建设提供了参考[19]。云安全基线的建设需要在传统安全基础上进行拓展，FedRAMP云安全基线是从传统环境下适用的NIST SP800－53《联邦信息系统和组织的安全及隐私控制》过渡到适应云计算环境安全控制的研究成果。

参考NIST SP800－53 r4和FedRAMP2.0，云计算环境下国家学术信息资源安全基线的构建至少需包含以下17类安全控制措施：访问控制、意识和培训、审计和可追究性、安全评估和授权、配置管理、应急规划、标识和鉴别、事件响应、维护、介质保护、物理和环境保护、规划、人员安全、风险评估、系统和服务采购、系统和通信保护、系统和信息完整性。每一类安全控制措施之下，都有若干个子类。NIST SP800－53 r4扩充了访问控制以及系统和服务采购的内容，以期覆盖云计算及供应链安全要求[4,20]。

云计算环境下国家学术信息资源安全基线的构建是一项复杂的系统工程，COBIT(Control Objectives for Information and Related Technology)是一个IT治理框架和支持工具集，管理者可以通过COBIT在信息安全控制目标、技术、风险之间建立关联，可以为信息安全控制提供明确的策略和实践指导。COBIT被用于作为制定和定义基线的基础，已经映射到很多信息安全标准中，很多组件都可以直接应用于云计算环境，也可以进行二次开发。云计算环境下国家学术信息资源安全基线的建立，需要结合云安全风险以及信息系统生命周期进行规划。云计算环境下学术信息资源服务机构需要降低安全风险，保障云服务信息系统的正常运行。学术信息资源服务机构以及云服务提供商必须应用现有的法律、标准、规范等进行安全控制措施的制定与选择，需要考虑云服务信息系统的安全、业务流程的安全实施、云服务环境安全等因素。云计算环境下国家学术信息资源安全基线应以业务系统为主，基于不同业务系统的特性进行不同的安全防护。同时将业务系统分解为不同的系统模块，如数据库、操作系统、网络设备等，根据业务层的定义进行安全控制细化，制定不同的安全控制基线。

云计算环境下国家学术信息资源安全基线建设，首先要区分不同安全需求所对应的基线要求，根据高、中、低3种不同的安全要求，构建3级云计算环境下国家学术信息资源安全基线。对于安全要求不在高、中、低之列的，主要从运行环境、运行特征、系统功能、威胁类型和信息类型等因素考量构建安全基线。此外，要明确安全控制措施的作用域，云信息安全基线并不是

控制措施越复杂越好，而需要考虑安全控制目标、运行环境、技术条件等因素，重视对云计算环境下国家学术信息资源关键业务和操作等方面的安全保障，从而进行合理的安全控制策略选择。

4.3 云计算环境下国家学术信息资源安全监测与应急响应

云计算环境下国家学术信息资源安全控制需对全过程信息安全进行监测，通过对信息安全相关活动和实践的数据收集，寻求最合理的安全控制方案，并在安全预测的基础上，实现安全事故的预警与应急响应，这样既能实现云计算环境下国家学术信息资源安全事故发生前的预防，也能实现事故发生后的控制。

云计算环境下国家学术信息资源安全监测主要是对云信息系统和云服务过程中的安全事件数据进行收集、分析和报告，主要涉及用户、应用程序和系统等活动信息，将收集的云信息安全相关数据进行汇集，从而为云计算环境下国家学术信息资源安全事件的评估提供量化的参考，更好地将安全事件控制在合理的范围内。云计算环境下国家学术信息资源安全监测及反馈过程[21]，如图 4 所示：

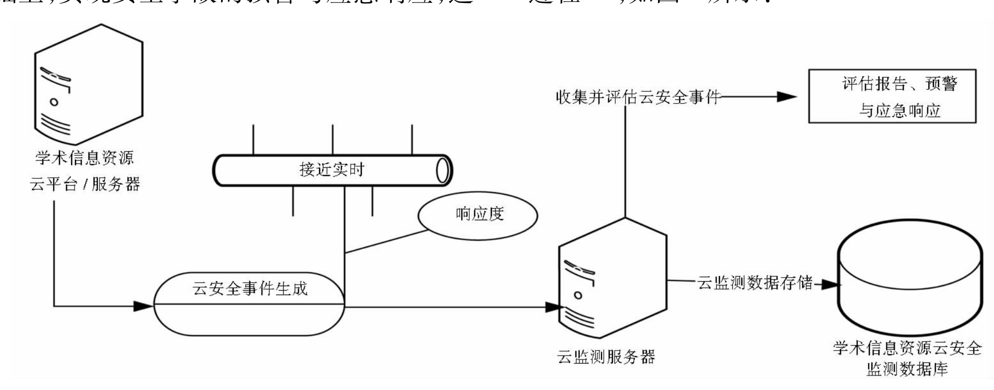


图 4 云计算环境下国家学术信息资源安全监测及反馈过程

云计算环境下国家学术信息资源安全监测作为云计算环境下国家学术信息资源安全控制策略的重要组成部分，主要作用在于可对安全风险进行检测。由于云计算技术的采用以及学术信息资源聚合，云计算环境下国家学术信息资源更容易成为攻击者的目标。有些攻击的发生无法事先预料，因此，对信息安全进行实时监测是对抗攻击和威胁的有效措施。可以通过对实时监测数据的收集、分析和评估采取及时的安全控制措施。

云计算环境下国家学术信息资源安全应急响应是整体安全防护循环上的一个重要环节。云计算环境下国家学术信息资源安全应急响应可以分为响应前、响应中和响应后 3 个阶段。响应前，主要在云计算环境下国家学术信息资源安全控制策略指导下，进行信息安全响应措施的制定。为了能够快速地响应、处理安全事故，需要制定安全事故处理的规程，并对安全事故进行分类。云计算环境下国家学术信息资源安全事故主要涉及系统故障、数据丢失与泄露、拒绝服务、不安全的 APIs 等。需要根据不同的安全事故类型制定应急预案，从而做好云计算环境下国家学术信息资源安全应急响应的准备。响应中，主要是基于云计算环境下国家学术信息资源安全监测的数据，找到安全问题，并利用信息安全的响应措施进行应对，防止被攻击者破坏从而将安全损失降到最低。响应后，主要是在事故处理完成后，及时修复国家学术信息资源的安全漏洞，巩固云计算环境下国家学术信息资源安全防护体系，并形成相应的报告以减少此类安全事故的发生，为相关责任人的责任追究提供证据。

云计算环境下国家学术信息资源安全应急响应在执行过程中，仍然需要人员的介入。通过人员参与将相对独立的策略、防护、监测、响应进行连接，并贯彻云计算环境下信息安全控制方案。因此，云计算环境下国家学术信息资源安全应急响应的实施需要对相关人员进行管理，提高相关人员的专业素质、以及应急响应问题的处理能力，以应对云计算环境下国家学术信息资源安全事故的动态变化，进行及时处理与防护，弥补应急响应模型及措施在执行过程中的不足。

4.4 云计算环境下国家学术信息资源安全合规审计

合规审计功能在传统的外包关系中发挥着重要作用。在云计算环境下，云服务提供商和学术信息资源服务机构面临着建立、监视一系列信息安全控制措施的持续合规性方面的挑战。云计算环境下合规与审计主要包含内部政策合规、法律合规和外部审计的协调作用，应从内部和外部流程实现需求目标的确立，明确

图书情报工作
第63卷 第7期 2019年4月

是否符合用户合同、法律法规、标准等规范；策略、程序、过程是否被实施以满足需求；监测策略、程序、过程是否被有效执行。

对于云服务提供商而言，在提供云服务的过程中必须遵守不同的IT流程控制需求，包括内部需求和外部需求。在实践过程中，众多的合规性要求形成了复杂的关系，在审计过程中或者安全事件的结果中难免会出现重复性的不合规控制，可以通过合规工作对这些内部需求和外部需求进行统一处理，从而提高效率并满足多组合的合规性要求。从长远发展来看，单个合规工作将被总体IT流程的合规取代。

合规需要和操作风险、内控进行有机结合，其中合规管理范围主要涉及外部监管法规和内部制度规程要求的合规事件。KPMG提出了通过合规审计构筑三道防线机制，其中第一道防线在于通过合规管理和内控，进行风险识别、评估、监测；第二道防线在于在强化合规管理和内控持续优化、风险缓释的基础上将三者进行优化组合；第三道防线在于对内部审计中使用的方法、流程和标准进行整合[22]。云服务提供商以及学术信息资源服务机构可以采用管理、风险和合规（GRC）概念，针对国家学术信息资源云安全建设过程中的云合规工作进行持续、正式的合规程序设计。

4.5 云计算环境下国家学术信息资源安全测评

云计算信息系统的安全测评主要是建立在传统信息系统安全评估的基础之上，云计算环境下国家学术信息资源安全测评，需要借鉴传统信息系统安全评估的流程与方法。传统信息系统安全测评经历了长期的发展，已经形成了一系列的规范和指南，从美国早期颁布的《可信计算机系统评估准则》[23]到英国颁布的信息安全管理实施规范（BS7799－1：1999）即ISO/IEC1799：2000[24]，再到美国颁布的联邦信息系统安全控制评估指南（SP800－53A）[25]等，都为云计算环境下的信息安全测评提供了参考。其中，《可信计算机系统评估准则》将安全保护能力划分为7个等级，为计算机安全测评提供了标准。由于公布时间较早，《可信计算机系统评估准则》关注技术上的不同需求，涉及信息访问控制以及保证，在目前新环境下不能有效扩展。ISO/IEC1799：2000主要为信息系统安全管理提供了一套体系，利用规划、执行、检查和整改过程提出了持续改进的管理模式，并详细列举了控制措施，为信息系统安全等级保护提供了指导。美国颁布的联邦信息系统安全控制评估指南（SP800－53A），提供了信息系统评估的方法、规程和建议，该概念框架明确了需要针对规范、行为、机制、人员四类对象进行测评。

云计算信息系统是信息系统发展的新模式，云计算环境下国家学术信息资源安全测评需要在传统信息系统测评的基础上发展，以适应云安全测评的变革。目前，云安全测评领域的研究仍在持续探讨之中。其中，在云计算环境下的隐私保护方面，美国发布了《联邦部门和机构使用云计算的隐私建议》，指出了云计算环境下隐私安全存在的风险，以及运用相关标准进行云计算环境下隐私安全风险的分析和评估；《公共云计算安全和隐私指南》分析公有云环境下相关威胁、风险，并提出了相应的保障措施，这两者为云安全测评的研究提供了重要参考。欧洲网络与信息安全局（ENISA）提出了信息安全保障框架，细化了云平台安全保障的指标，为云安全测评工作提供了指导。云安全联盟（CSA）提出了云安全控制矩阵3.0，提出云供应商的基本安全原则，用来指导和协助云客户的整体安全风险评估，并提供了一个涉及16个领域的控制框架，该控制框架横跨了其他行业标准与法律法规。

总体而言，云安全测评尚未形成统一的测评体系，各个组织机构在传统信息系统安全测评的基础上进行了一些探索，目前研究主要集中于云服务提供商安全能力要求、云计算平台安全等标准研究。云计算应用于国家学术信息资源存储和服务，需要通过持续的云安全测评，以减少学术信息资源服务机构采纳云计算的风险，提高整体的安全防护能力。云计算环境下国家学术信息资源安全测评，需要克服云计算技术带来的诸多挑战，主要包括：虚拟化、数据安全、应用安全、物理安全、多租户、系统安全、网络安全。与传统信息系统安全测评环境不同的是，云计算环境下国家学术信息资源安全测评，需要在大规模应用技术异构、物理和虚拟环境混合、大量租户共享的环境下进行云安全测评工作。

我国从颁布《中华人民共和国计算机信息系统安全保护条例》到等级保护全面推广，传统信息系统的安全测评标准已经经历了较长时间的发展，形成了相对成熟的等级测评体系，为云计算环境下国家学术信息资源安全测评工作的开展奠定了良好的基础。安全等级测评是信息系统安全测评领域较为成熟的方法，该方法以国家颁布的相关标准为测评依据，面向的主体对象是信息系统。在参考传统信息系统安全等级测评过程的基础上[26－28]，构建云计算环境下国家学术信息资源安全测评工作流程，见图5。

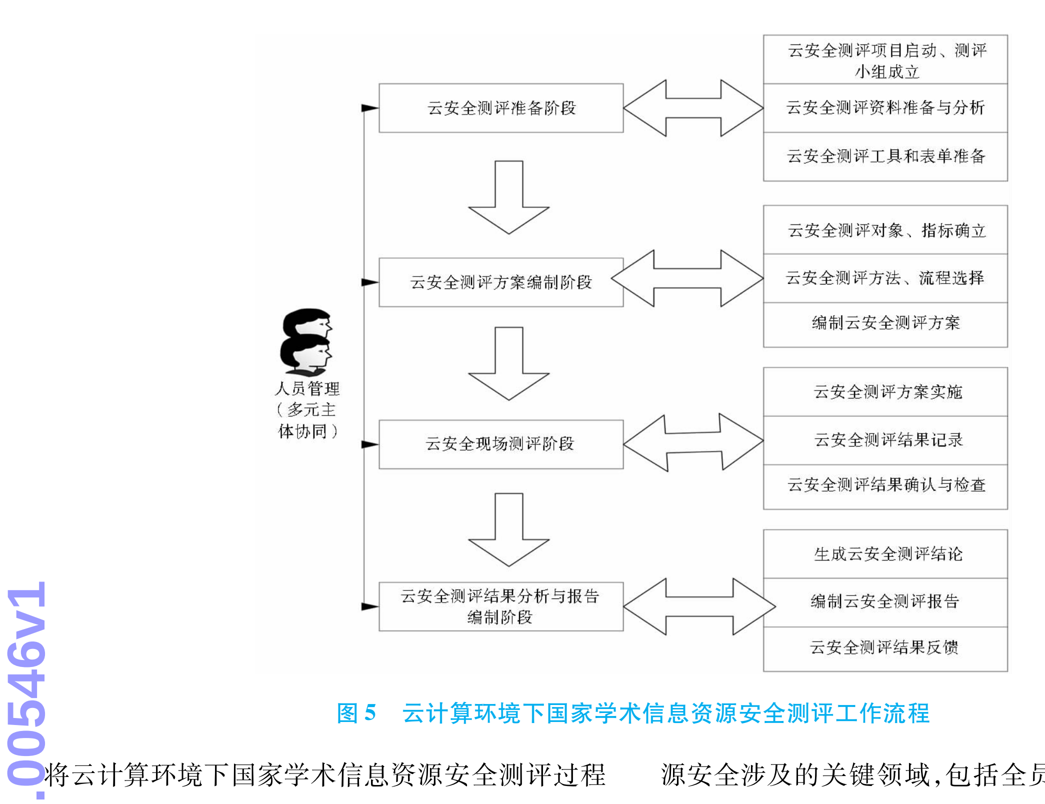


图 5　云计算环境下国家学术信息资源安全测评工作流程

将云计算环境下国家学术信息资源安全测评过程分为 4 个阶段：云安全测评准备阶段、云安全测评方案编制阶段、云安全现场测评阶段以及云安全测评结果分析与报告编制阶段。云计算环境下国家学术信息资源安全测评准备阶段主要完成测评项目启动工作，成立相关的测评小组，通过资料搜集掌握国家学术信息资源云信息系统的现状，为测评方案的编制提供参考；在云安全测评方案编制阶段，进一步确定云安全测评的内容，制定云安全测评方案；云安全现场测评阶段主要完成测评方案的内容，进行测评结果的记录；云安全测评结果分析与报告编制阶段主要是根据现场测评的结果进行分析和总结，在此基础上生成云安全测评报告并进行反馈。在整个云安全测评过程中，需要云计算环境下国家学术信息资源服务参与方多元主体协同，在沟通协调的基础上，完成相关的测评工作，以保障云安全测评的效果。

5　结语

在借鉴传统复杂系统安全控制论的人、机、环有机整体以及信息保障技术框架的人、操作、技术的模式基础上，结合云计算环境下信息安全控制关键域与治理域，构建云计算环境下国家学术信息资源安全控制框架。云计算环境下国家学术信息资源安全控制既包括云计算环境下国家学术信息资源安全控制措施，同时包括对云计算环境下国家学术信息资源安全控制措施的有效性测量。通过对云计算环境下国家学术信息资源安全涉及的关键领域，包括全员管理、控制策略、安全测评予以分析，并提出优化措施，为云计算环境下国家学术信息资源安全保障组织与实施提供参考。

参考文献：

[1] 王惠莅，杨晨，张明天，等. SP800 系列信息安全标准研究[J]. 信息技术与标准化，2011 (5)：65－69.

[2] ISO/IEC－27003(CN)信息技术－安全技术 信息安全管理体系实施指南[EB/OL]. [2018－07－04]. https://wenku.baidu.com/view/53ff26b6dd36a32d737581dd.html.

[3] 温克勒. 云计算安全：架构、战略、标准与运营[M]. 刘戈舟，等译. 北京：机械工业出版社，2012.

[4] Security and Privacy Controls for Federal Information Systems and Organizations[EB/OL]. [2018－07－04]. http://go.thalesesecurity.com/rs/480-LWA-970/images/NIST-Special-Publication-800-53-Revision-4.pdf.

[5] ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services [EB/OL]. [2018－07－17]. https://www.iso.org/standard/43757.html.

[6] ISO/IEC 27017 Extending ISO/IEC 27001 into the Cloud [EB/OL]. [2018－07－17]. https://www.bsigroup.com/Documents/iso-27017/resources/ISO-27017-overview.pdf.

[7] FedRAMP. Security Assessment Framework [EB/OL]. [2018－07－17]. https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/01/FedRAMP-Security-Assessment-Framework-v2-1.pdf.

[8] CSA CCM V3.0.1[EB/OL]. [2018－07－17]. https://cloudsecurityalliance.org/search/? s=Cloud+Controls+Matrix+v3.0.1.

[9] CAIQ (Consensus Assessments Initiative Questionnaire)[EB/OL]. [2018-10-21]. https://searchcloudsecurity.techtarget.com/definition/CAIQ-Consensus-Assessments-Initiative-Questionnaire.
[10] Security guidance for critical areas of focus in cloud computing v3.0 [EB/OL]. [2018-07-17]. https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf.
[11] 胡昌平,吕美娇. 云环境下国家学术信息资源安全保障组织研究现状与问题[J]. 情报理论与实践, 2017, 40(11):10-16.
[12] 王瑛 汪送. 复杂系统风险传递与控制[M]. 北京:国防工业出版社,2015.
[13] 虞文进,李健俊. 基于IATF思想的网络安全设计和建设[J]. 信息安全与通信保密, 2010(1):122-125.
[14] 云安全控制矩阵 ccm 中英文版[EB/OL]. [2018-06-29]. https://max.book118.com/html/2018/0303/155631961.shtm.
[15] 赵彦龙. UCDRS 系统的功能特点及其在图书馆联合参考咨询服务网络中的应用[J]. 数字图书馆论坛,2006(7):66-68.
[16] 胡俊荣. 构建跨系统联合数字参考咨询服务网络平台[J]. 图书情报工作,2006,50(5):83-87.
[17] 陈驰,于晶,等. 云计算安全体系[M]. 北京:科学出版社,2014.
[18] 王祯学. 信息系统安全风险估计与控制理论[M]. 北京:科学出版社,2011.
[19] 赵章界,刘海峰. 美国联邦政府云计算安全策略分析[J]. 信息网络安全,2013(2):1-4.
[20] 周亚超,左晓栋. 网络安全审查体系下的云基线[J]. 信息安全与通信保密,2014(8):42-44.
[21] 李天枫,姚欣,王劲松. 大规模网络异常流量实时云监测平台研究[J]. 信息网络安全, 2014(9):1-5.
[22] KPMG 银行业操作风险研讨会. 操作风险管理及与内控、合规管理的有机结合[EB/OL]. [2018-06-29]. https://wenku.baidu.com/view/8c790dfe03d276a20029bd64783e0912a2167c98.html? from = search.
[23] Trusted Computer System Evaluation Criteria[EB/OL]. [2018-06-29]. https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria.
[24] BS7799-1:1999 信息安全管理[EB/OL]. [2018-06-29]. http://doc.mbalib.com/view/8448db6df953cf0870802975331ebf51.html.
[25] NIST Special Publication 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations [EB/OL]. [2018-06-29]. https://www.nist.gov/itl/nist-cloud-computing-related-publications.
[26] 信息安全技术 信息系统安全等级保护测评过程指南[EB/OL]. [2018-06-29]. http://tds.antiy.com/biaozhun/6/index.html.
[27] 肖国煜. 信息系统等级保护测评实践[J]. 信息网络安全,2011,36(7):86-88.
[28] 杨磊,郭志博. 信息安全等级保护的等级测评[J]. 中国人民公安大学学报(自然科学版), 2007,13(1):50-53.

作者贡献说明:
万莉:撰写论文初稿,修改论文;
胡昌平:提出选题,指导论文写作。

Control and Management of National Academic Information Resources Security in Cloud Computing Environment

Wan Li[1] Hu Changping[2]
[1] School of Journalism & Communication, Nanchang University, Nanchang 330031
[2] School of Information Management, Wuhan University, Wuhan 430072

Abstract: [**Purpose/significance**] In order to provide references for national academic information resources security, this paper aims to construct the security control framework for national academic resources in cloud computing environment. [**Method/process**] Based on Human-Machine-Environment organic unity in safety control theory of conventional complexity system, and Information Assurance Technical Framework that combines "the people, the operation, the technology", this paper integrates the key domain and governance domain in information security guarantee to construct the above security control framework. [**Result/conclusion**] Under the cloud computing environment, the key domains in the national academic information resources security include personnel management, control strategy, and safety assessment. The framework contains not only the national academic information resources security strategy, but also effectiveness measurements of it.

Keywords: academic information resources security control security management information resource security